BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

VAIT-Novelle und Ausgliederungen an Cloud-Anbieter

Andreas Pfeßdorf, Referat GIT 4
IT-Prüfungen und Prüfungsunterstützung

Jochen Zengler, Referat VA 54
Grundsatz Governance und Risikomanagement/Schnittstelle IT-Aufsicht

Agenda

- VAIT-Novelle 2022
  - ✓ Hintergründe der Novellierung
  - ✓ Umsetzung der Novellierung
  - ✓ Wesentliche Änderungen und Konkretisierungen
- Ausgliederungen an Cloud-Anbieter
  - ✓ Regulatorik
  - ✓ Europäischer und nationaler Ansatz
  - ✓ Prüfung von Cloud-Verträgen

VAIT-Novelle 2022

Beweggründe für die Überarbeitung

- Umsetzung der EIOPA-Leitlinie zu Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologien (ICT-Guidelines)
- Ergänzungs- und Aktualisierungsbedarf aus der Prüfungspraxis und verschiedenen Gremien
- Redaktionelle Anpassungen

Wesentliche Änderungen:

- Neue Kapitel „Operative Informationssicherheit“ und „IT-Notfallmanagement“
- Konkretisierung der Anforderungen insbesondere beim Informationsrisiko- und Informationssicherheitsmanagement, Berechtigungsmanagement sowie bei IT-Ausgliederungen

VAIT-Novelle 2022

Vorgehen bei der Novellierung

- Abgleich der Leitlinien von EBA und EIOPA und Identifizierung des Anpassungsbedarfs der BaFin-Rundschreiben VAIT und BAIT
- Redaktionelle Änderungen
- Einbindung des Fachgremiums IT (BAIT) und des Expertengremiums IT (VAIT)
- Öffentliche Konsultationen
- Konsolidierung und Berücksichtigung der Stellungnahmen bei der Finalisierung der Rundschreiben
- Veröffentlichung: 3. März 2022

Was sind Fachgremien?

- Sie setzen sich aus Vertreterinnen und Vertretern der Aufsicht und der beaufsichtigten Unternehmen sowie deren Verbänden zusammen.
- Sie dienen dem regelmäßigen Austausch zu aktuellen Themen und der frühzeitigen Kommunikation/ Information.

VAIT-Novelle 2022

Grundprinzipien unverändert

- Prinzipienorientiert
- Proportionalitätsprinzip
- Bauen auf gesetzlichen Vorgaben und teilweise auf Rundschreiben auf.
- Gängige Standards sind zu beachten.

VAIT – ergänzt & konkretisiert insbesondere Regelungen aus den einschlägigen VA-Rundschreiben

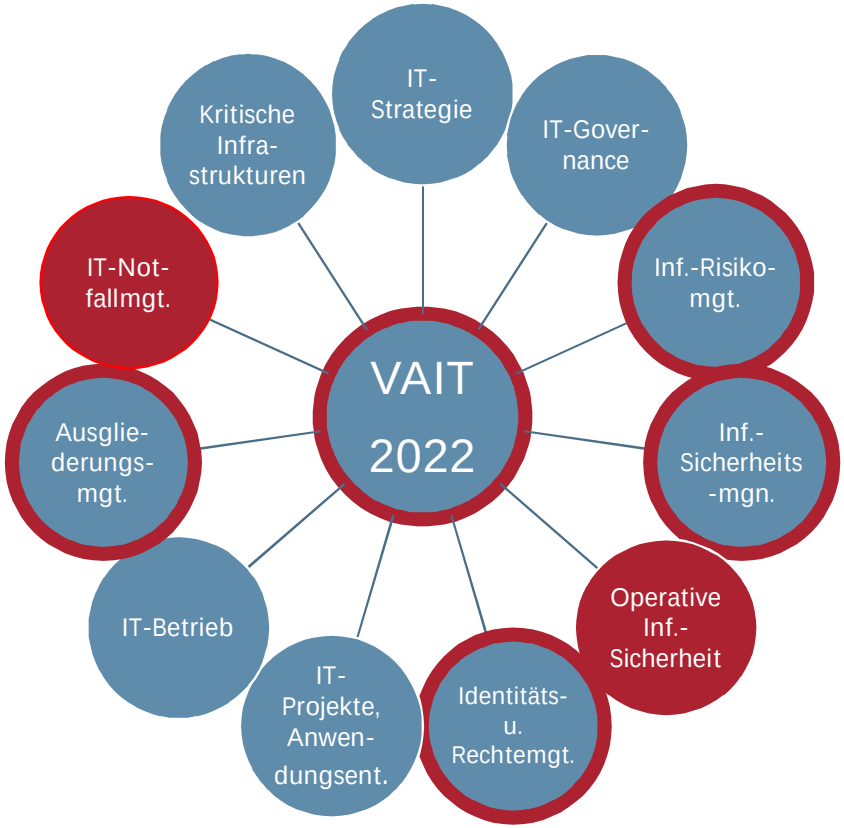
- RS 02/2017 „Aufsichtsrechtliche Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGO)
- RS 01/2020 „ Aufsichtsrechtliche Mindestanforderungen an die Geschäftsorganisation von kleinen Versicherungsunternehmen nach § 211 VAG (MaGo für kleine VU)
- RS 08/2020 „ Aufsichtsrechtliche Mindestanforderungen an die Geschäftsorganisation von Einrichtungen der betrieblichen Altersvorsorge (MaGo für EbAV)

VAIT-Novelle 2022

Überblick

Wesentliche Änderungen:

- Neue Kapitel „Operative Informationssicherheit“ und „IT-Notfallmanagement“
- Konkretisierung der Anforderungen insbesondere beim Informationsrisiko- und Informationssicherheitsmanagement, Berechtigungsmanagement sowie bei IT-Ausgliederungen

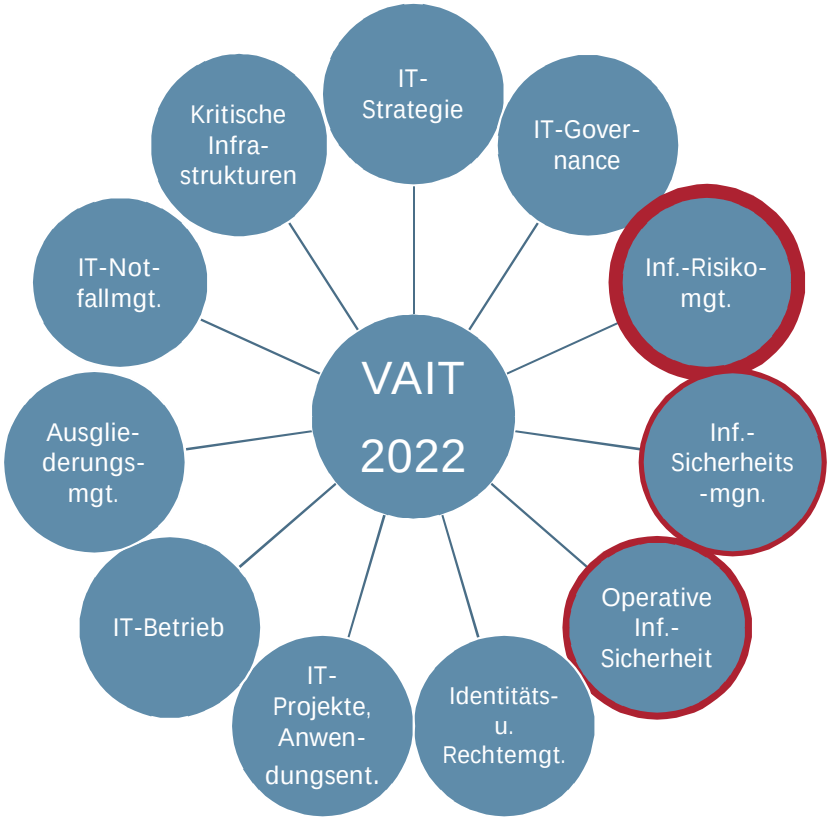


VAIT-Novelle 2022

Anforderungen aus dem Informationsrisikomanagement

- Informationsverbünde und Ermittlung des Schutzbedarfs inklusive deren Abhängigkeiten und Schnittstellen mit Dritten
- Information der Geschäftsführung bzw. des Vorstandes über die Ergebnisse und über Veränderungen der Risikosituation unter anderem einschließlich externer potenzieller Bedrohungen

- <u>Neu Textziffern bzw. Ergänzungen:</u>
  - Stärkere Einbeziehung der Eigentümer von Informationen und Prozessen (Tz. 3.5)
  - Überprüfung der Schutzbedarfsfeststellung durch Informationsrisikomanagement (Tz. 3.6)
  - Beobachtung der Bedrohungslage/Schwachstellen des Informationsverbundes und ggf. Veranlassung geeigneter Maßnahmen (Tz. 3.9)

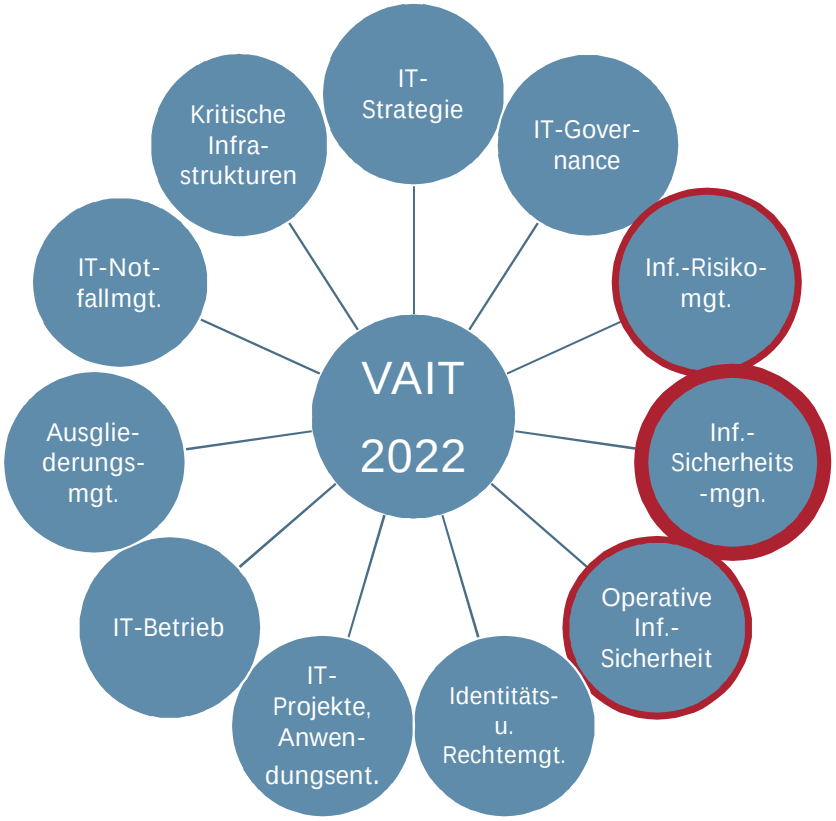


VAIT-Novelle 2022

Anforderungen aus dem Informationssicherheitsmanagement

- Informationssicherheitsleitlinien
- Überwachung der Einhaltung der Informationssicherheitsvorgaben
- Funktion des Informationssicherheitsbeauftragten (Neu: ISB aktivere Einbindung bei IT-Projekten Tz. 4.5)
- Initiiert und koordiniert Maßnahmen, die zur Gewährleistung der Informationssicherheit notwendig sind

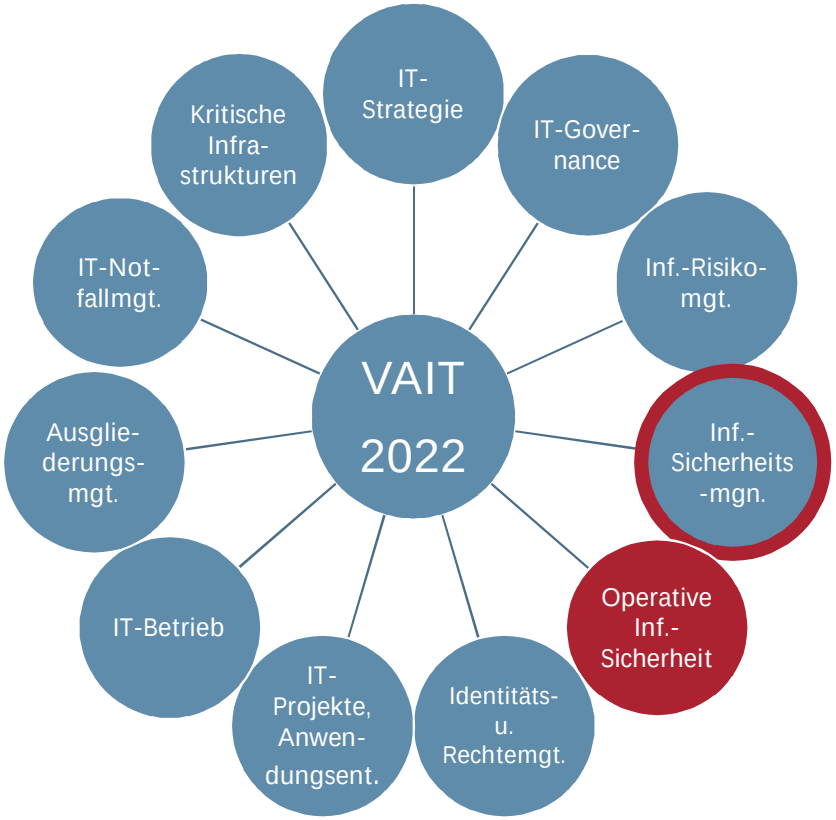
- <u>Neu als separate Textziffern:</u>
  - Wirksamkeitsüberprüfung der Soll-Maßnahmen: Richtlinie über das Testen und Überprüfen der Maßnahmen zum Schutz der Informationssicherheit (Tz. 4.4)
  - Sensibilisierungs- und Schulungsprogramm für Informationssicherheit (Tz. 4.9)



VAIT-Novelle 2022

Neues Kapitel „Operative Informationssicherheit“

- Die Informationssicherheit ist ein zentrales Thema in den VAIT.
- Durch Unterteilung in zwei Kapital werden die Anforderungen weiter konkretisiert und die Bedeutung der Informationssicherheit erhöht.
- Informationssicherheitsmanagement
  => Grundlegende Anforderungen an die Überwachung der Informationssicherheit
- Operative Informationssicherheit => Tagesgeschäft
- Beispiele für Maßnahmen benannt, die zur Umsetzung der Anforderungen aus dem Informationssicherheitsmanagement geeignet sind



VAIT-Novelle 2022

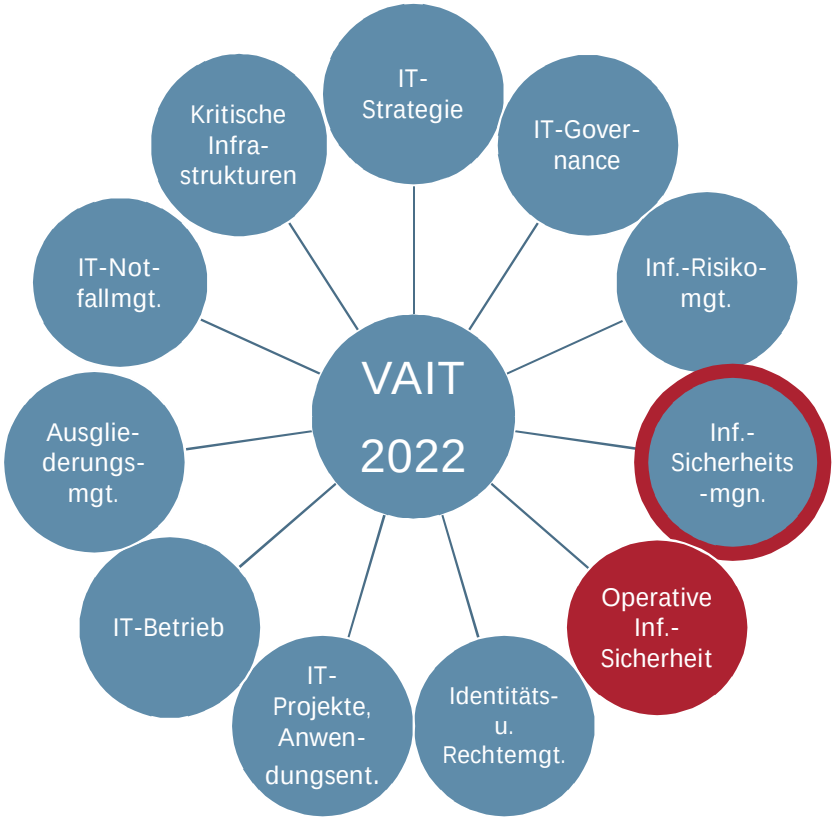
Neues Kapitel „Operative Informationssicherheit“

Umsetzung der Anforderungen des Informationssicherheitsmanagements

- Dem Stand der Technik entsprechende Informationssicherheitsmaßnahmen und Prozesse implementieren (Tz.5.2)

- Regelbasierte Erkennung von Sicherheitsvorfällen; Security Information and Event Management (SIEM) (Tz. 5.3 bis 5.5)

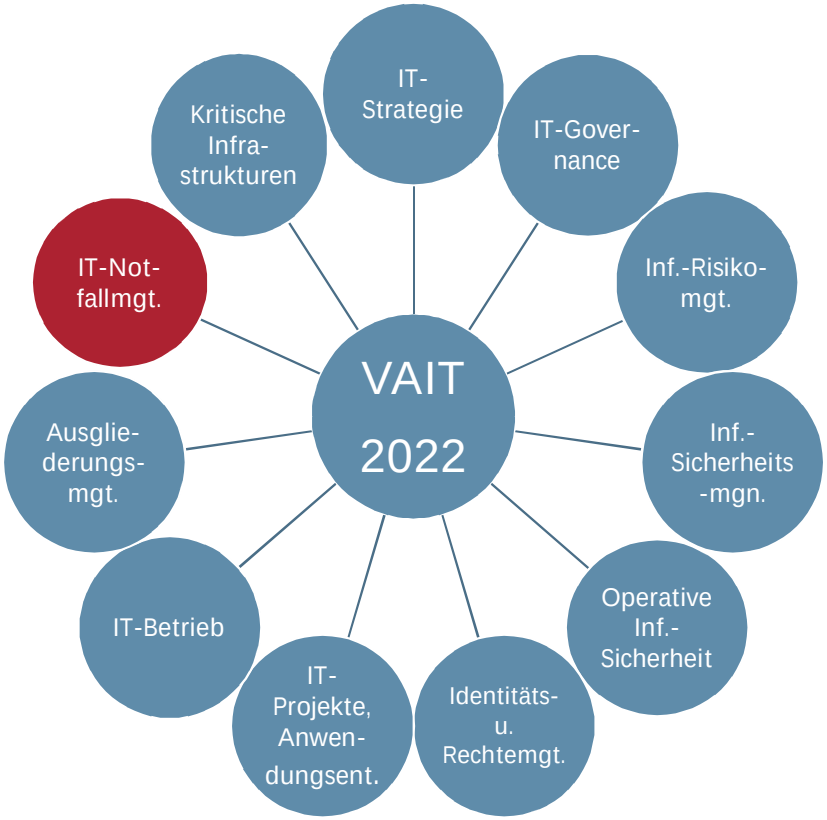
- Laufende Überprüfung der Sicherheit der IT-Systeme (Tz. 5.6)



VAIT-Novelle 2022

Neues Kapitel „IT-Notfallmanagement“

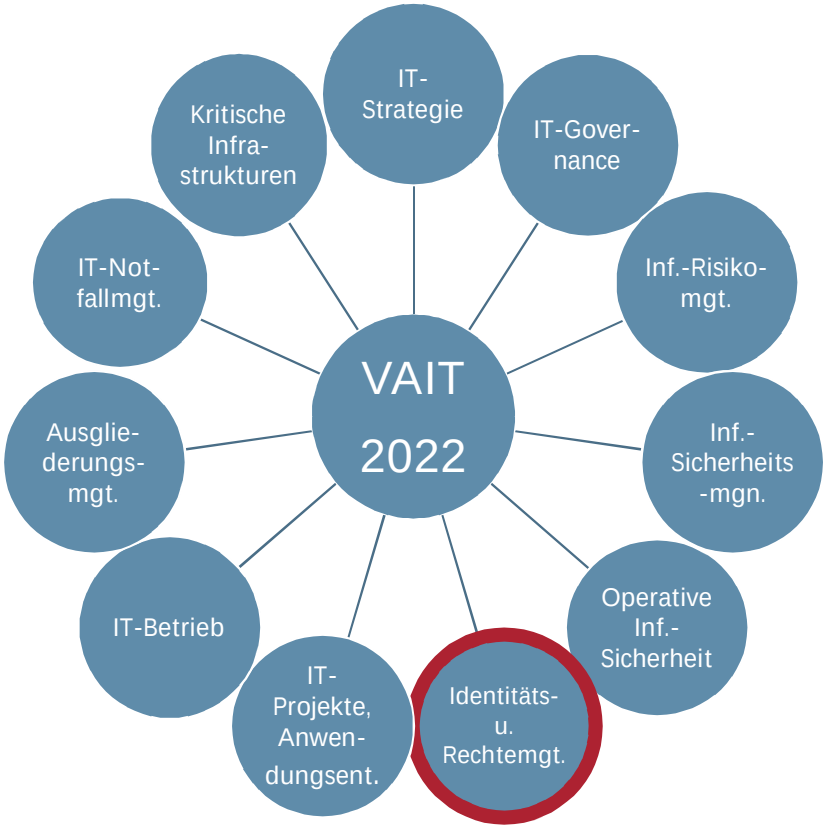
- Ziele und Rahmenbedingungen bauen auf allgemeines Notfallmanagement auf.
- IT-Notfallpläne sind für alle IT-Systeme mit zeitkritischen Aktivitäten/Prozessen zu erstellen.
- IT-Notfalltests (auf Basis eines IT-Testkonzeptes) überprüfen jährlich ihre Wirksamkeit.
- Nachweis zu erbringen für hinreichend langen IT-Notbetrieb aus anderem Rechenzentrum



VAIT-Novelle 2022

Weitere Änderungen: Kapitel „Identitäts- und Rechtemanagement“

- Identitäts- und Rechtemanagement umfasst jegliche Art von Zugriffs-, Zugangs- und Zutrittsrechten.
- Jede Berechtigung muss einer handelnden bzw. verantwortlichen Person zugeordnet sein.
- Präzisierung des Sparsamkeitsgrundsatzes („Need-to-know“- & „Least-Privilege“-Prinzipien)
- Regelmäßige & anlassbezogene Überprüfung von Berechtigungskonzepten
- Protokollierung und Überwachung privilegierter Berechtigungen



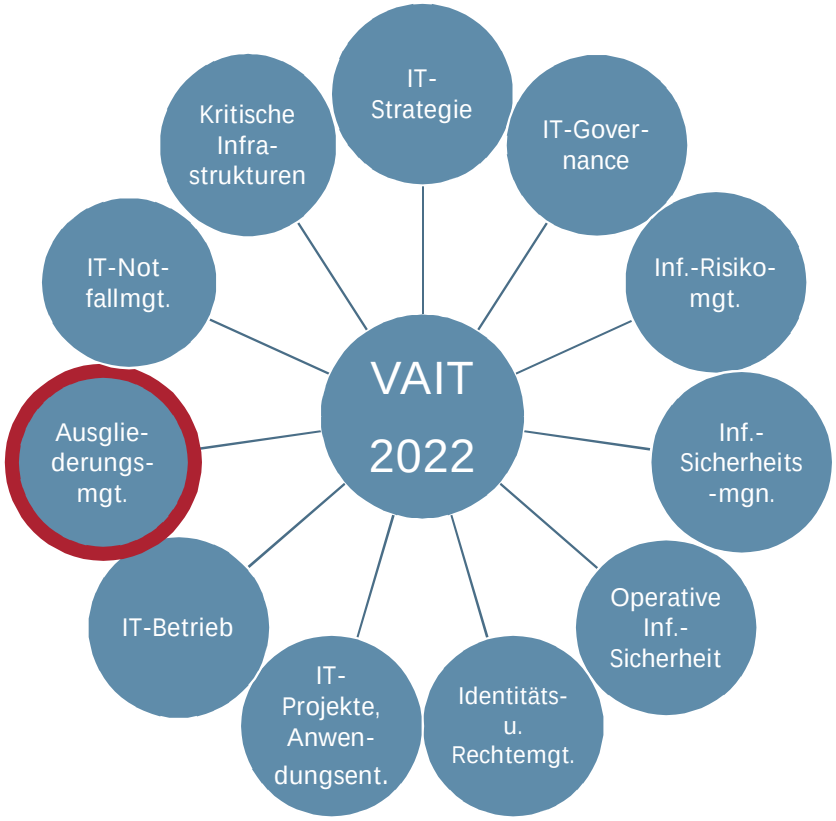
VAIT-Novelle 2022

Weitere Änderungen:
„Ausgliederungsmanagement“

Konkretisierungen in der Vorbemerkung:

- VU muss bei Ausgliederung an IT-Dienstleister die Einhaltung der VAIT-Anforderungen durch den IT-Dienstleister vertraglich sicherstellen.

- IT-Dienstleister können auch Trägerunternehmen von Einrichtungen der betrieblichen Altersvorsorge sein.



Agenda

- VAIT-Novelle 2022
  - ✓ Hintergründe der Novellierung
  - ✓ Umsetzung der Novellierung
  - ✓ Wesentliche Änderungen und Konkretisierungen
- Ausgliederungen an Cloud-Anbieter
  - ✓ Regulatorik
  - ✓ Europäischer und nationaler Ansatz
  - ✓ Prüfung von Cloud-Verträgen

1. Vor- und Nachteile der Cloudnutzung

Vorteile

- Niedrige Nutzungskosten
- Geschwindigkeit (Bereitstellung & Computing)
- Skalierbarkeit
- Höhere Produktivität durch Auslagerung von Wartungsarbeiten und Nutzung von Frameworks etc.
- Zugriff auf neue Technologien (KI, ML etc.)
- Resilienz
- Höhere Sicherheit der Cloud (im Verantwortungsbereich der Cloud Service Providers (CSPs)

Nachteile

- Oftmals zusätzliche Belastungen in Migrationsphase durch Altverträge
- Mangelnde Kontrolle
- Lock-In-Effekt
- Juristische Herausforderungen im Bereich Datenschutz bei der Nutzung von nicht-EU CSPs („US-Cloud-Act“ vs. GDPR)
- Erhöhte Anforderungen an die Sicherheit in der Cloud (im Verantwortungsbereich des Nutzers)
- Risiko von Datenabfluss an den CSP

2. Regulatorik

Handlungsbedarf im aufsichtlichen Umgang mit Cloud-Anbietern

- Geschäftsbereichsübergreifend wird die steigende Nutzung von Cloud-Anbietern verzeichnet.
- US-Tech-Unternehmen stehen an der Spitze.
- Ausgliederungen in die Cloud, insbesondere an die US-amerikanischen Cloud-Anbieter, stellen Unternehmen und Aufsicht zugleich vor neue Herausforderungen.
- BaFin hat in den vergangenen Jahren die Probleme identifiziert und Lösungen erarbeitet.

3. Kommunikation mit Cloud-Anbietern

- Regelmäßige Teilnahme an Regulatory Summits von Cloud-Anbietern
- Bilaterale Gespräche der BaFin mit Cloud-Anbietern zu den Anforderungen an Ausgliederungen nach den deutschen Aufsichtsgesetzen
- Einwirken auf eine aufsichtsrechtskonforme Gestaltung der finanzmarktspezifischen Zusatzvereinbarungen zu den Ausgliederungsverträgen, insbesondere mit Blick auf die in der Orientierungshilfe genannten Aspekte
- Abstimmung aufsichtsrechtskonformer Zusatzvereinbarungen, jedoch ohne abschließende Freigabe

4. Europäische Ansätze: Cloud Guidelines & DORA

Guidelines der ESAs zu Ausgliederungen an Cloud-Anbieter:

- EBA: Guidelines on outsourcing arrangements (EBA/GL/2019/02) und die darin integrierten Recommendations on outsourcing to cloud service providers (EBA-Rec-2017-03)
- EIOPA: Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002)
- ESMA: Guidelines on outsourcing to cloud service providers (ESMA50-157-2403)

Entwurf des Digital Operational Resilience Act (DORA) (Verhandlungsmandat des Rates):

- IKT-Drittparteirisikomanagement
- Oversight Framework für kritische IKT-Drittdienstleister

5.1 Nationaler Ansatz: BaFin- Orientierungshilfe & FISG

- BaFin hat im November 2018 das Merkblatt Orientierungshilfe für Auslagerungen an Cloud-Anbieter (auch auf Englisch) veröffentlicht.
- Aufsichtliche Einschätzung zur Ausgliederung an Cloud-Anbieter und der Einhaltung der damit verbundenen aufsichtsrechtlichen Anforderungen; bestehende Anforderungen an Ausgliederungen bleiben unberührt
- Keine neuen Anforderungen
- Orientierungshilfe ist nicht verbindlich, daher oft als Empfehlung („soll“/ „sollte“) formuliert.
- Überarbeitung in 2022 geplant

5.2 Nationaler Ansatz: BaFin-Orientierungshilfe & FISG

- Neuer Rahmen zur Überwachung von Cloud-Anbietern durch Regelungen zu Ausgliederungen im Gesetz zur Stärkung der Finanzmarktstabilität (FISG)

- (Wieder-)Einführung der Anzeigepflicht für wesentliche Auslagerungen (zum Beispiel im Kreditwesengesetz
- Unmittelbare Informations- und Prüfrechte gegenüber Ausgliederungsunternehmen

- Pflicht zur vertraglichen Vereinbarung eines inländischen Zustellungsbevollmächtigten des Ausgliederungsunternehmens mit Sitz in Drittstaat

- Geschäftsbereichsübergreifend: Anzeigenverordnungen

6. Prüfung von Cloud-Ausgliederungsverträgen

- BaFin-Orientierungshilfe zu Auslagerungen an Cloud-Anbieter als Hilfestellung
- Strategische Überlegungen: Unternehmen sollen
  - Überlegungen zur Nutzung von Cloud-Diensten in ihrer IT-Strategie abbilden,
  - Prozesse entwickeln und dokumentieren, die alle für die Ausgliederung an den Cloud-Anbieter relevanten Schritte von der Strategie über die Migration in die Cloud bis hin zur Exit-Strategie abdecken,
  - vor Ausgliederung zunächst alle relevanten internen Prozesse dahingehend überprüfen, ob diese bereit für „die Cloud“ sind, insbesondere
    - ✓ auszulagernde Sachverhalte und
    - ✓ Risikomanagement- und -steuerungsprozesse.

7. Prüfung von Cloud-Ausgliederungsverträgen

Risikoanalyse:

- Prüfung, inwieweit die aufsichtsrechtlichen Anforderungen an Ausgliederungen zu beachten sind.
- (Nicht abschließende) Aufzählung wesentlicher Inhalte der Risikoanalyse, zum Beispiel:
  - ✓ Bewertung der Risiken, die sich aus dem gewählten Dienstleistungsmodell/ Bereitstellungsmodell ergeben können,
  - ✓ eine Bewertung der finanziellen, operationellen Risiken einschließlich der rechtlichen Risiken sowie Reputationsrisiken; dazu zählen auch Erwägungen zum Standort der Datenspeicherung und der Datenverarbeitung,
  - ✓ Bewertung der Eignung des Cloud-Anbieters (Know-how, Infrastruktur, wirtschaftliche Situation, gesellschaftsrechtlicher und regulatorischer Status etc.).

8. Praxisbeispiel zur Risikoanalyse

Prüfung von Exit- und Alternativszenarien im Falle einer vorzeitigen bzw. außerplanmäßigen Beendigung einer Cloudausgliederung

- In welchem Umfang ist ein „Customizing“ erfolgt? → Individualisierung erschwert Migration
- Ist ein „Lock-In-Effekt“ eingetreten? Ist eine vollständige Abbildung der gewünschten Umgebung bei einem anderen Anbieter oder In-House noch möglich?
- Ist die Exit-Strategie tatsächlich vorhanden – liegt also eine verschriftlichte und durchdachte Exit-Strategie vor, die zum Beispiel potentielle Ausweichsysteme und Anbieter umfangreich beschreibt?
- Lässt die für eine Migration veranschlagte Zeit darauf schließen, dass Schnittstellen und Datenaustauschformate neu konzipiert werden müssen? → Bei einer Exit-Strategie sollten diese Überlegungen bereits vor Eintritt des Szenarios bekannt und anwendbar sein.

9. Cloud-Prüfungen

- Erleichterung bei den Prüfungen großer Cloud-Anbieter:
- Sammelprüfungen: Prüfungen eines Cloud-Anbieters werden von mehreren beaufsichtigten Unternehmen gemeinsam organisiert und von diesen (oder von ihnen beauftragten Dritten) gesammelt durchgeführt.
- „Dienstleister-Modell“: Mehrere Unternehmen wählen gemeinsam einen Dienstleister aus.
- Prüfressourcen können auf diese Weise sowohl bei den beaufsichtigten Unternehmen als auch bei den Cloud-Anbietern effizienter gebündelt und damit Kosten gespart werden.
- Nachweise/Zertifikate auf Basis gängiger Standards (zum Beispiel Internationaler Sicherheitsstandard ISO/IEC 2700X, C 5-Anforderungskatalog des BSI), Prüfberichte anerkannter Dritter oder interne Prüfberichte des Cloud-Anbieters

10. Fazit

- Auch zukünftig Herausforderungen für Aufsicht und beaufsichtigte Unternehmen

- BaFin begleitet regulatorische Vorhaben aktiv auf nationaler, europäischer und internationaler Ebene.

- Überwachung von Ausgliederungsunternehmen mit Fokus auf US-amerikanischen Cloud-Anbieter durch FISG und DORA wird Finanzstabilität stärken und Unternehmen entlasten.

Andreas Pfeßdorf
Referat GIT 4
IT-Prüfungen und Prüfungsunterstützung
Telefon: +49(0)2284108-7692
E-Mail: andreas.pfessdorf@bafin.de

Jochen Zengler
Referat VA 54
Grundsatz Governance und Risikomanagement/
Schnittstelle IT-Aufsicht
Telefon: +49(0)2284108-7359
E-Mail: jochen.zengler@bafin.de

Bildnachweis: pixabay.com/geralt